00227 "Th8h760

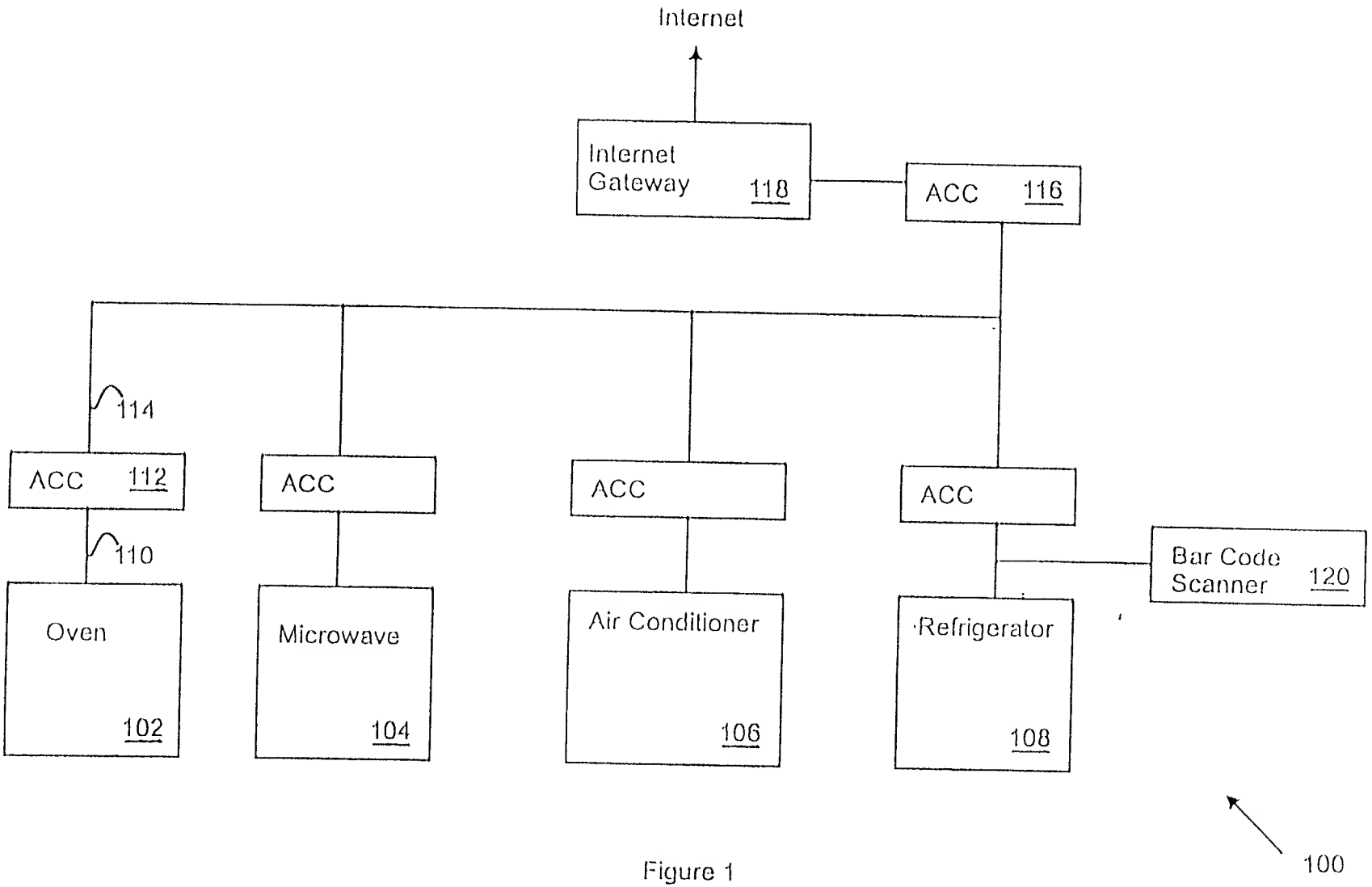

Figure 1

00232T "TTTBTT260

STX	RX ADD	TX ADD	NUM BYTES	CMD	MFG	APPL TYPE	DATA	CRC	ETX
8	16	16	16	16	16	16	Variable	12	8

200

Figure 2

STX	RX ADD	RX ADD	TX ADD	TX ADD	TX ADD	NUM BYTES	CMD	MFG	APPL TYPE	DATA	CRC	ETX
	14FF	FC12	12FF	3EFF	C254							

302 304

300

Figure 3

STX	RX ADD	TX ADD	NUM BYTES	CMD			MFG	APPL TYPE	DATA	CRC	ETX
				Community	Field	Command					
8	16	16	16	4	4	8	16	16	Variable	12	8

400

Figure 4

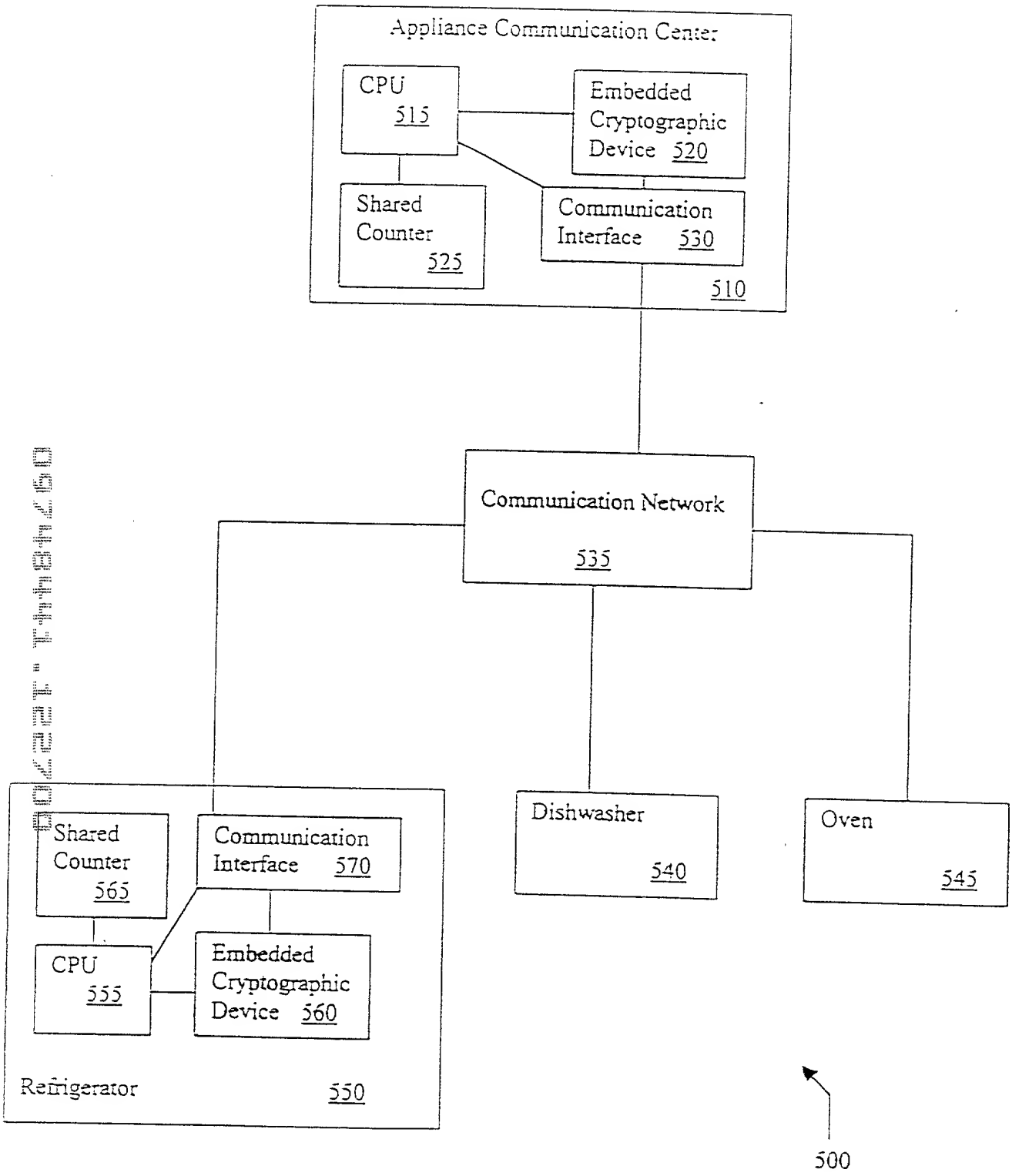
Appliance Communication Center
CPU
515
Embedded
Cryptographic
Device 520
Shared
Counter
525
Communication
Interface 530
510
Communication Network
535
Shared
Counter
565
Communication
Interface 570
CPU
555
Embedded
Cryptographic
Device 560
Refrigerator 550
Dishwasher
540
Oven
545
500

Figure 5

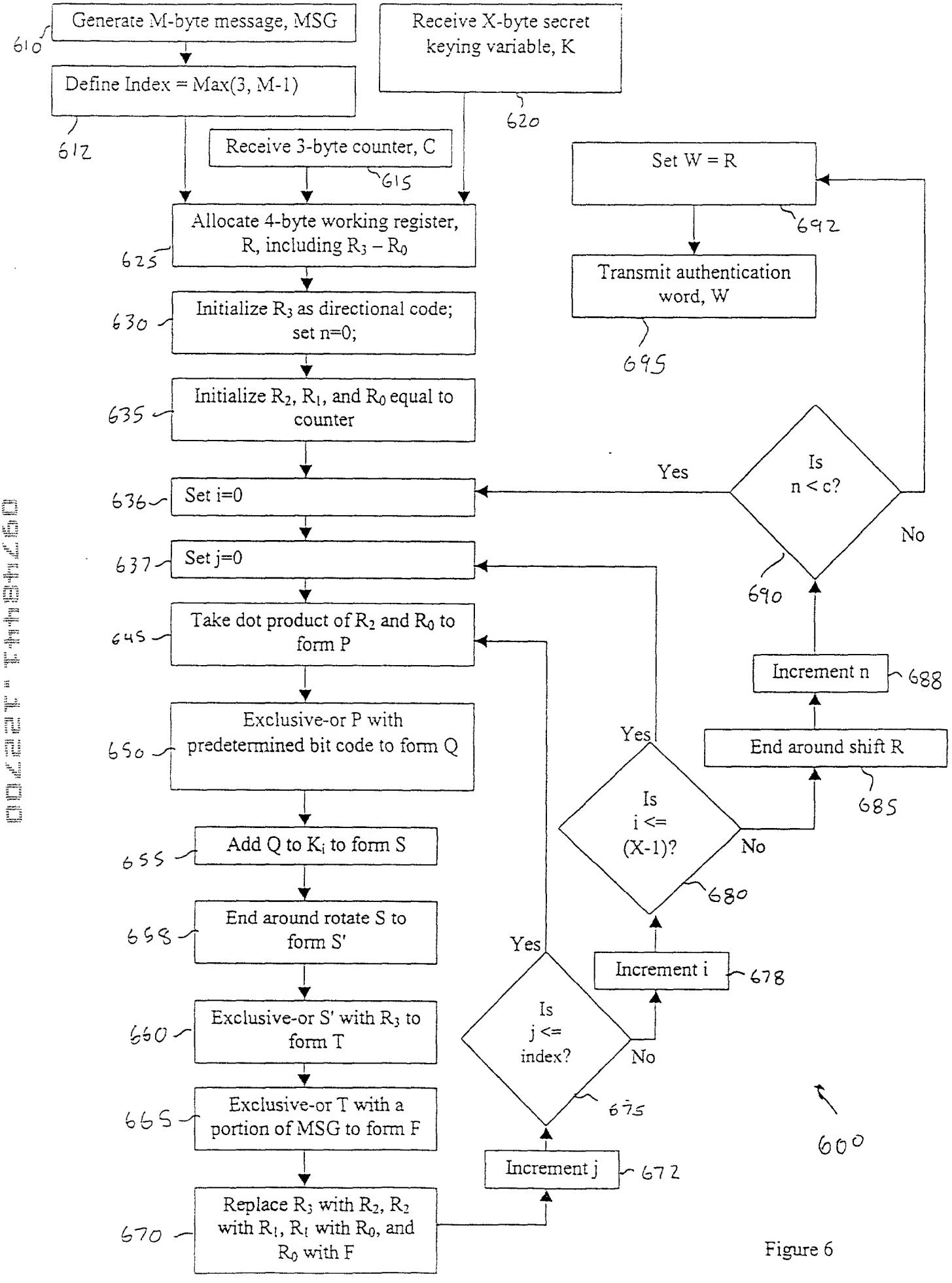
Generate M-byte message, MSG
610
Receive X-byte secret keying variable, K
620
Define Index = Max(3, M-1)
612
Receive 3-byte counter, C
615
Allocate 4-byte working register, R, including $R_3 - R_0$
625
Initialize R_3 as directional code; set n=0;
630
Initialize R_2, R_1, and R_0 equal to counter
635
Set i=0
636
Set j=0
637
Take dot product of R_2 and R_0 to form P
645
Exclusive-or P with predetermined bit code to form Q
650
Add Q to K_i to form S
655
End around rotate S to form S'
658
Exclusive-or S' with R_3 to form T
660
Exclusive-or T with a portion of MSG to form F
665
Replace R_3 with R_2, R_2 with R_1, R_1 with R_0, and R_0 with F
670
Increment j
672
Is j <= index?
675
Yes
No
Increment i
678
Is i <= (X-1)?
680
Yes
No
End around shift R
685
Increment n
688
Is n < c?
690
Yes
No
Set W = R
692
Transmit authentication word, W
695
600

Figure 6

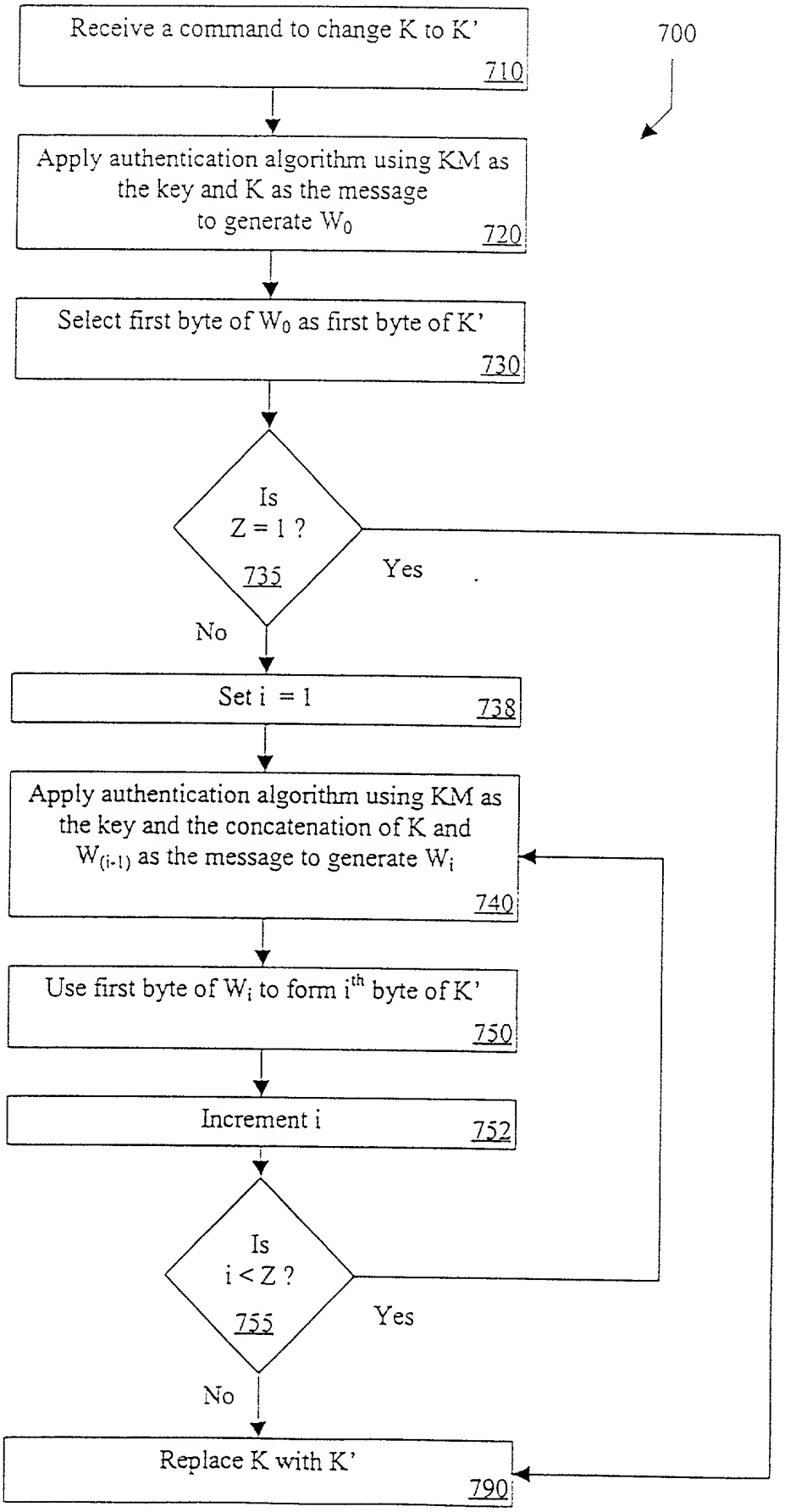
Receive a command to change K to K'
710
700
Apply authentication algorithm using KM as the key and K as the message to generate W_0
720
Select first byte of W_0 as first byte of K'
730
Is Z = 1 ?
735
Yes
No
Set i = 1
738
Apply authentication algorithm using KM as the key and the concatenation of K and $W_{(i-1)}$ as the message to generate W_i
740
Use first byte of W_i to form i^{th} byte of K'
750
Increment i
752
Is i < Z ?
755
Yes
No
Replace K with K'
790

Figure 7

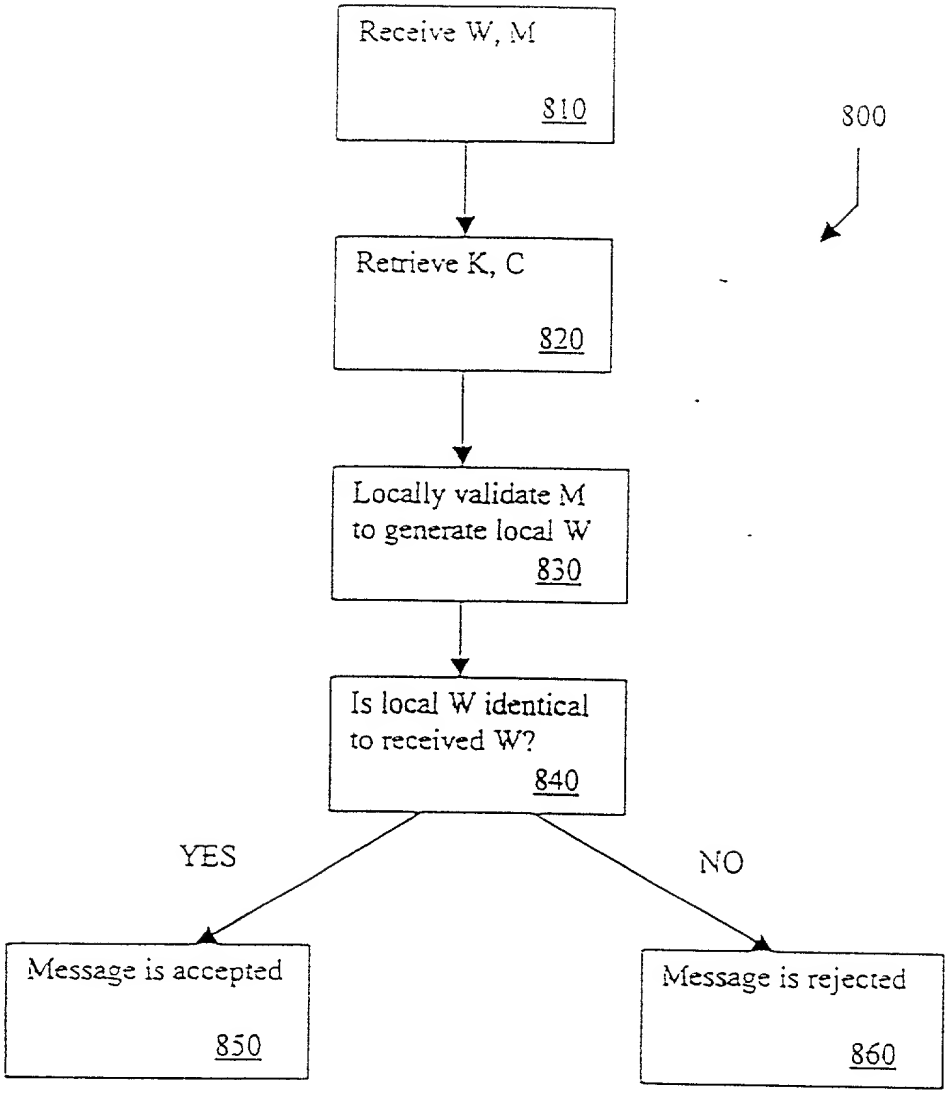
Receive W, M
810
800
Retrieve K, C
820
Locally validate M
to generate local W
830
Is local W identical
to received W?
840
YES
NO
Message is accepted
850
Message is rejected
860

Figure 8